General Server Farm Security Requirements

SERVER FARM OPEN STORAGE AREA GENERAL REQUIREMENTS TO SECRET LEVEL

The following have been extracted from the Communications Security (COMSEC) Material Control System (CMS21A) and edited to include requirements from SECNAVINST 5510.36

(Indicates requirements taken from SECNAVINST 5510.36, CHAPTER 10)

ANNEX O

CONSTRUCTION SPECIFICATIONS FOR FIXED COMSEC(OPEN STORAGE AREA) FACILITIES

1. **Purpose:** To prescribe minimum construction requirements for fixed COMSEC facilities.

2. **Construction Requirements:** A fixed COMSEC facility must be constructed of solid(permanent construction materials; i.e. plaster, gypsum wallboard, metal panels, hardboard, wood, plywood), strong materials that will deter and detect unauthorized penetration. It must provide adequate attenuation of internal sounds that would divulge classified information through walls, doors, windows, ceilings, air vents, and ducts.

3. **Walls, Floors, and Ceilings:** Walls, floors, and ceilings shall be of sufficient structural strength to prevent or reveal any attempts at unauthorized penetration.

a. Walls shall be constructed from true floor to true ceiling.

b. Ceilings shall ideally be at least as thick as the outer walls and offer the same level of security as the outer walls.

c. Where false ceilings are used, additional safeguards will be required to resist unauthorized entry (e.g., installation of an approved intrusion detection system (IDS) in the area above the false ceiling).

4. **Doors and Entrance Areas:** Only one door shall be used for regular entrance to the facility. Other doors may exist for emergency exit and for entry or removal of bulky items.

a. All doors shall remain closed during facility operations and should only be opened to admit authorized personnel or material.

b. The following standards apply to facility doors and entrance areas:

(1) **Main entrance door:**

(a) Design and Installation: The access door must be of sufficient strength to resist forceful entry.

GSA-approved vault doors,

Standard 1-3/4 inch, internally reinforced, hollow metal industrial doors, **or**

Metal-clad or solid hardwood doors with a minimum thickness of 1-3/4 inch.

(b) The door frame must be securely attached to the facility and must be fitted with a heavy-duty/high security strike plate and hinges installed with screws long enough to resist removal by prying. (The hinge pins of outswing doors shall be peened, brazed, or spot welded to prevent removal.)

(c) The door shall be installed to resist the removal of hinge pins. This can be accomplished by either installing the door so that the hinge pins are located inside the facility or by set screwing/welding the pins in place.

(2) **Door lock:** The main entrance door to facilities which are not continuously manned must be equipped with a GSA-approved electro-mechanical lock meeting Federal Specification FF-L-2740.

(a) For facilities which are continuously manned, a built-in lock is not required; however, the door must be able to accommodate a combination electro-mechanical lock meeting Federal Specification FF-L-2740 and dead bolt should it ever become necessary to lock the facility from the outside (e.g., in case of emergency evacuation).

(b) An electronically activated lock (e.g., cipher lock or keyless push-button lock) may be used on the entrance door to facilitate the admittance of authorized personnel when the facility is operationally manned. However, these locks do not afford the required degree of protection and may not be used to secure the facility when it is not manned.

NOTE: Facilities equipped with a GSA-approved, built-in Group 1R lock prior to 01 July 1993 may continue to use the Group 1R lock.

(3) **Other doors:** Other doors (e.g., emergency exit doors and doors to loading docks) must meet the same installation requirements as the main facility entrance doors and must be designed so that they can only be opened from inside the facility. (They shall be secured from the inside by a dead bolt lock, panic dead bolt lock, or rigid wood or metal bar which extends across the width of the door. Key operated locks that can be accessed from the exterior side of the door are not authorized.)

Emergency escape mechanisms that by-pass the built-in combination lock should be double-latched. All doors must remain closed during facility operations and must be opened only for passage of authorized personnel or material.

NOTE: Approved panic hardware and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the interior surfaces of other doors to the facility.

(4) **Entrance areas:** The facility entrance area shall be equipped with a device which affords personnel desiring admittance the ability to notify personnel within the facility of their presence.

(a) A method shall be employed to establish positive visual identification of a visitor before entrance is granted.

(b) The entrance area shall be designed in such a manner that an individual cannot observe classified activities until cleared for access into the restricted spaces.

5. **Windows:** COMSEC facilities should not normally contain windows. Where windows exist, they shall be secured in a permanent manner to prevent them from being opened. The protection provided to the windows need be no stronger than the strength of the contiguous walls.

a. Windows that are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, shall be constructed from or covered with materials that will provide protection from forced entry. Facilities located within fenced and guarded government compounds or equivalent may eliminate this requirement. If the windows are made inoperable by either sealing them or equipping them on the inside with a locking mechanism.

b. Observation of internal operations of the facility shall be denied to outside viewing by covering the windows from the inside or otherwise screening the secure area from external viewing.

6. **Other openings:** Air vents, ducts, or any similar openings which breach the walls, floor, or ceiling of the facility shall be appropriately secured to prevent penetration.

a. Openings which are less than 96 square inches shall have approved baffles installed to prevent an audio or acoustical hazard.

b. If the opening exceeds 96 square inches, acoustical baffles shall be supplemented by either hardened steel bars or an approved intrusion detection system (IDS).

ANNEX P

"SPECIAL" PHYSICAL SECURITY SAFEGUARDS
FOR DOD BLACK BULK FACILITIES

1. **Purpose:**

a. To delineate the physical security safeguards which are unique to those facilities operated by or for the DoD, and employ classified crypto-equipment to protect multichannel trunks passing encrypted or unclassified information, and otherwise referred to as DoD bulk facilities.

b. The area within a structure occupied by a DoD Bulk facility is referred to as a "space," and it is this "space" that requires the safeguards prescribed in this Annex. The structure which contains the space is referred to as a "site."

2. **Construction Requirements:**

a. **Walls**: At sites which are not continuously manned, walls shall be of solid (permanent) construction from true floor to true ceiling and shall be constructed in such a manner that attempts at unauthorized penetration will be detected or prevented. (Walls shall be extended to the true ceiling with permanent construction materials, wire mesh, or 18-guage expanded steel screen.)

b. **Doors:** Only one door should be used for regular entrance to the facility. The door must be strong enough to resist forceful entry. At sites which are not continuously manned, the entrance door shall be of substantial material (e.g., metal clad or solid wood with a minimum thickness of 1 and 3/4-inch, hinged from inside, fitted with a GSA approved electromechanical lock meeting Federal Specification FF-L-2740).

NOTE: Sites fitted with GSA-approved, built-in Group 1R locks with dead bolt extensions, or a heavy duty hasp and GSA-approved padlock prior to 01 July 1993 do not have to retrofit with electro-mechanical locks meeting Federal Specification FF-L-2740.

(1) Other doors may exist for emergency exits and moving bulky items. The doors must meet the construction criteria of the main entrance door and must be designed to open from inside the facility only. Approved panic hardware, intrusion detection, and locking devices (lock bars, dead bolts, knobs, or handles) may be placed only on the interior surfaces of other doors to the facility. Emergency escape mechanisms that bypass the built-in combination lock should be double-latched.
All doors must remain closed during facility operations and must be opened only for passage of authorized personnel or material.

(2) A built-in lock is not required for sites continuously manned; however, the main entrance door must be able to accommodate a combination electromechanical lock meeting Federal Specification FF-L-2740 and dead bolt should it ever become necessary to lock the facility from the outside.

c. **Windows:** Where windows exist affording visual surveillance of personnel, documents, materials, or activities within the site, the windows shall be made opaque or equipped with blinds, drapes, or other coverings precluding such visual surveillance. Windows less than 18 feet above the ground, measured from the bottom of the window, or are easily accessible by means of objects directly beneath the window, must be protected from forced entry. All perimeter windows at ground level (less than 18 feet above the ground) shall be covered by an IDS.

d. **Access Control**

(1) During duty hours, the site entrance should be under visual control at all times to preclude entry by unauthorized personnel. This may be accomplished by several
methods (e.g. employee work station, guard, CCTV). Regardless of the method utilized, an access control system shall be used on the site entrance. Persons not appropriately cleared shall be continuously escorted within the space by an appropriately cleared person who is familiar with security procedures. Authorized personnel who permit another individual to enter the space are responsible for confirming the individual's access and need-to-know.

(2) An automated access control system may be used to control admittance to the site during working hours in lieu of visual control, if it meets the criteria stated below.

(a) The automated access control system must identify an individual and authenticate that person's authority to enter the space through the use of an identification (ID) badge or card, or by personal identity verification. The ID badge or card must use embedded sensors, integrated circuits, magnetic stripes or other means of encoding data that identifies the site and the individual to whom the card is issued.

(b) In conjunction with the ID badge or card above, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device and consist of four or more digits, randomly selected, with no logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

(c) Personal identity verification (Biometrics Device) identifies the individual requesting access by some unique characteristics such as: fingerprinting, hand geometry, handwriting, retina, or voice recognition.

NOTE: A procedure must be established for removal of the individual's authorization to enter the site/space upon reassignment, transfer or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than required.

e. **Daily Security Checks**

(1) In a continuously manned site, there should be a visual check once per shift ensuring all COMSEC material is properly safeguarded and physical security systems or devices (e.g. door locks and vent covers) are functioning properly.

(2) In a site not continuously manned, the security check shall be conducted prior to departure of the last person. The check should ensure all COMSEC material is properly stored, that security containers are properly secured, and the space is secured against unauthorized access. The last person to depart shall ensure the entrance door to the site is locked and intrusion detection systems are activated.

f. **Intrusion Detection System (IDS):**

(An IDS must detect an unauthorized or authorized penetration in the secure area. An IDS complements other physical security measures and consists of Intrusion Detection Equipment, Security Forces and Operating procedures.)

(1) Sites which are not continuously manned shall be equipped with an approved IDS. Either U.S. or Allied personnel may be assigned to monitor the IDS and to direct the responding guard(s). An IDS must detect an attempted or actual human entry into the protected area. An IDS complements other physical security measures and consists of three essential components: intrusion detection equipment, security and response force personnel, operation procedures. Details of installed IDS shall be controlled and restricted on a need-to-know basis.

(a) Intrusion Detection Equipment (IDE). Primary power for all IDE will be commercial AC or DC power. The system should have an emergency backup power system, which may consist of either battery and/or generator power complying with underwriter laboratory (UL-603) specifications and must alarm in an attended area, where a guard can be dispatched within five minutes.

(b) Alarm Condition Response. Every alarm condition will be treated initially as a detected intrusion until resolved by the response force. The response force will investigate the source of an alarm (e.g. intrusion, tampering, component or system power failure) and will notify site personnel. The response force will take appropriate steps to safeguard the site and prevent the escape of an intruder from the site as permitted by SOP, local law enforcement, and circumstances until properly relieved. Tests of the response force must be conducted semiannually. Results of investigations by the response force will be maintained at the monitor station.

(c) Operating Procedures. A written support agreement must be established for external monitoring and/or response.

(2) IDS sensors will be tested semiannually. The IDS will incorporate a means for providing historical record of all events, either automatically or through the use of a manual log system. If the IDE does not have a provision for automatic entry into an archive, the operator will record the time, source, and type of alarm, and action taken. The historical record must be routinely reviewed and retained by the command security officer. Records of alarm annunciation shall be retained for at least 90 days or until investigations of system violations and incidents have been successfully resolved and recorded.